Oracle Optimized Solution for Secure Oracle WebLogic Server

ORACLE WHITE PAPER | OCTOBER 2015

Table of Contents

Introduction 1

Integrated Enterprise Application Stack 2

Oracle Solaris 11 2

Oracle Solaris Zones 3

Oracle VM Server for SPARC 3

Oracle WebLogic Server 12*c* 3

Oracle’s SPARC Servers 3

A Comprehensive Approach to Security 3

Because Oracle can innovate, integrate, and test at all levels of the technology stack, it is in a unique position to provide a comprehensive security approach at the solution level. More details on the security aspects of this particular solution are provided below under “Understanding Oracle WebLogic Server Security.” 4

Solution Architecture 4

Physical Architecture 5

Virtual Architecture 5

Tuning Guidelines 6

Performance Expectations 7

CPU and Memory Utilization 8

Sizing and Role Guidelines 8

Security: SPARC Processor Cryptography Acceleration 9

SPARC Cryptography Performance 10

Understanding Oracle WebLogic Server Security 11

Java EE Security Feature Support in Oracle WebLogic Server 11

Overview of the Oracle WebLogic Server Security Service 11

Oracle WebLogic Server Security Framework 11

Managing Oracle WebLogic Server Security 12

Security Realms 13

Security Policies 13

Oracle Platform Security Services 13

Conclusion 13

For More Information 15

Introduction

Oracle WebLogic Server has long set the enterprise standard for a secure, high-performance, high availability, and high-value application server platform. Oracle Optimized Solution for Secure Oracle WebLogic Server builds upon this success, providing a pretested and optimized architecture for deploying enterprise Java applications. Employing this pretested and preconfigured infrastructure can help mitigate risk, reduce complexity, and accelerate the deployment of new applications.

Oracle Optimized Solutions provide build instructions and best practices for assembling best-of-breed combinations of Oracle's servers and storage products, Oracle applications, and the Oracle Solaris operating system. Oracle's hardware and software engineers work together to integrate the complete technology stack and to ensure that Oracle applications, databases, and middleware are optimized with compute capacity, storage, networking, and operating systems. This approach also delivers extreme performance, availability, and security while greatly simplifying deployment and support.

This document focuses on the configuration and performance characteristics of Oracle Optimized Solution for Secure Oracle WebLogic Server on Oracle's latest SPARC servers. The paper describes the solution architecture, illustrates a test environment used to gather performance characterization information, and provides sizing guidelines. Details about Oracle WebLogic Server security are also provided, along with recommended optimizations for achieving a reliable solution.

Solution Overview

Oracle Optimized Solution for Secure Oracle WebLogic Server features a complete infrastructure for deploying Oracle WebLogic Server version 12*c* in an enterprise environment. The sections that follow describe the integrated enterprise application stack and the underlying hardware components required for Oracle WebLogic clusters that demonstrate high availability.

Performance and availability expectations, sizing recommendations, and results were partly derived from the most recent record-setting performance testing conducted using the SPECjEnterprise benchmark standards. While the architecture of the solution described in this paper departs from the test environment specified in the formal benchmark test, Oracle's testing provides a more sophisticated expression of the system's capabilities that is more applicable to common deployment scenarios. The approach takes advantage of unique Oracle product features for enhancing availability and properly sizing a configuration, as well as focusing on cost-effectiveness and practicality.

This solution described in this paper concentrates on core features and common deployment scenarios. It omits certain details about less commonly used configuration options of Oracle Database and some Oracle WebLogic features, with unique customer-specific options left open to the end user. Large amounts of related documentation already exist, including a dedicated Oracle Optimized Solution for deploying complementary Oracle Database solutions. Platform-specific features are highlighted where they provide significant benefits to deployment performance or security. In particular, features of Oracle's latest SPARC M7 processor can be used to particular advantage.

Note: *While Oracle WebLogic Server forms a core part of the of the Oracle Fusion Middleware portfolio, the information in this paper is relevant only to Oracle WebLogic Server.*

Integrated Enterprise Application Stack

Oracle Optimized Solution for Secure Oracle WebLogic Server provides a complete environment for deploying Java Platform, Enterprise Edition (Java EE) applications. The solution utilizes an integrated enterprise application stack that includes the Oracle Solaris 11 operating system, built-in virtualization, and Oracle WebLogic Server. Security is considered an integral part of this solution—at every level of the application stack—resulting in a comprehensive approach that competitive solutions can't match.

Oracle Solaris 11

The Oracle Solaris 11 operating system includes innovative functionality, such as near wire-speed networking security and high availability features that deliver resiliency and industry-leading performance. Built-in virtualization features help to optimize resource utilization, and advanced security features provide the isolation and control required by enterprise environments. Oracle Solaris Zones and Oracle VM Server for SPARC (formerly called Sun Logical Domains) are both described in this architecture to securely and conveniently host and deploy Java EE applications. Some of the major features of the Oracle Solaris 11 operating system include

» High-performance 64-bit operating environment
» Support for large memory and high-CPU-count systems
» Excellent scalability for highly threaded Java applications
» Predictive Self Healing, a feature designed to keep applications up and running
» Extensive instrumentation and diagnostic capabilities to assist performance and availability
» Integrated specialized security features leveraging CPU cryptographic features

Oracle Solaris Zones

Oracle Solaris Zones allow kernel-level separation of applications running in a single Oracle Solaris 11 instance. As an included feature of the Oracle Solaris 11 operating system, Oracle Solaris Zones technology provides built-in, no-added-cost virtualization. Oracle Solaris Zones are rapid to deploy, impose extremely low overhead, and are used in this solution to separate instances of Oracle WebLogic Server.

Oracle VM Server for SPARC

Oracle VM Server for SPARC (formerly called Sun Logical Domains), allows OS- and hardware-level isolation of application environments running separate Oracle Solaris 11 instances within a server platform. Oracle Solaris Zones can be nested within logical domains (LDoms) to allow organizations to take advantage of the benefits of both features. Oracle VM Server for SPARC is provided as a built-in feature of Oracle Solaris on SPARC platforms. This no-added-cost virtualization technology provides extremely low overhead isolation of hardware and operating environments.

Oracle WebLogic Server 12*c*

Oracle WebLogic Server 12*c* is a fully compliant Java EE application server that is feature-rich and holds benchmark world records for Java EE performance. Oracle WebLogic Server 12*c* takes full advantage of the 64-bit addressable memory and also the large number of hardware threads available in servers such as Oracle's SPARC M7 processor–based servers, as described in this solution.

Oracle's SPARC Servers

Oracle's new SPARC M7 processor–based servers run Oracle Solaris 11, with Oracle Solaris 10 supported in guest LDoms or zones only. Both operating systems have demonstrated excellent performance and security running Java applications for enterprise workloads. SPARC M7 processor–based servers are especially ideal for deploying Java applications on Oracle WebLogic Server, due to their optimally balanced single-threaded and multithreaded performance capabilities as well as integrated hardware accelerators for encryption and database queries. Older Java applications that were coded for and performed well on single-threaded, clock-speed-centric servers can operate happily alongside their more-modern, multithreaded counterparts.

Options for running Oracle WebLogic Server within the SPARC server family include Oracle's new SPARC T7-1, T7-2, T7-4, M7-8, and M7-16 servers as well as earlier generations of Oracle's SPARC T5 and SPARC T4 processor–based servers. The SPARC M7 processor–based systems scale to a maximum configuration of up to sixteen 4.13-GHz processors[1], up to 8 TB of memory, and up to eight internal SAS or high-performance solid-state devices (SSDs) or NVM Express (NVMe) drives. If required, extremely high bandwidth can also be provided to both network and external storage devices.

A Comprehensive Approach to Security

Security has become paramount as more and more web-based applications access personal or business-critical information. Because more sensitive data is now exchanged across the internet, security must be a major priority when designing and deploying a web services environment. As a result, securing data both in-flight and statically is paramount. Protecting the internal infrastructure from intrusions and ensuring the integrity of digital information has also become a priority and a core business function for most organizations.

[1] Each SPARC M7 processor provides up to thirty two cores per processor and eight threads per core, for a maximum of 4,096 threads.

Oracle Optimized Solutions are designed to address key security challenges, including

- **Complexity**. Complexity breeds insecurity, and the security of any implementation as a whole will only be as strong as its weakest component. It can be very difficult to understand how to securely implement the myriad products included in a web services deployment. Oracle Optimized Solutions offer guidelines and recommendations to simplify deployments using best practices, consolidation, and virtualization technologies.
- **Implementation flaws**. Secure software is important but not sufficient for comprehensive systemic security. Most security vulnerabilities stem from flawed implementation or architecture, improper configuration, improper access control, lack of adequate patch management, unencrypted communications, or inadequate policies and processes. Oracle Optimized Solutions provide proven and tested architecture recommendations that follow existing security best practices and recommendations, dramatically reducing risk.
- **Performance and cost**. Often the implementation of security settings and requirements can have a significant negative impact on a system's performance and cost. For example, on-the-fly encryption—required for effective security—can significantly impact performance for production systems, or it can require expensive computational add-ons. Oracle Optimized Solutions offer high-performance security by using cryptographic accelerators directly implemented into SPARC processor cores. This innovation results in wire-speed security capabilities without the performance penalties and cost barriers typically associated with real-time secure computing.

Because Oracle can innovate, integrate, and test at all levels of the technology stack, it is in a unique position to provide a comprehensive security approach at the solution level. More details on the security aspects of this particular solution are provided below under "Understanding Oracle WebLogic Server Security."

Solution Architecture

Figure 1 and the sections that follow describe the physical and virtual architecture of Oracle Optimized Solution for Secure Oracle WebLogic Server.

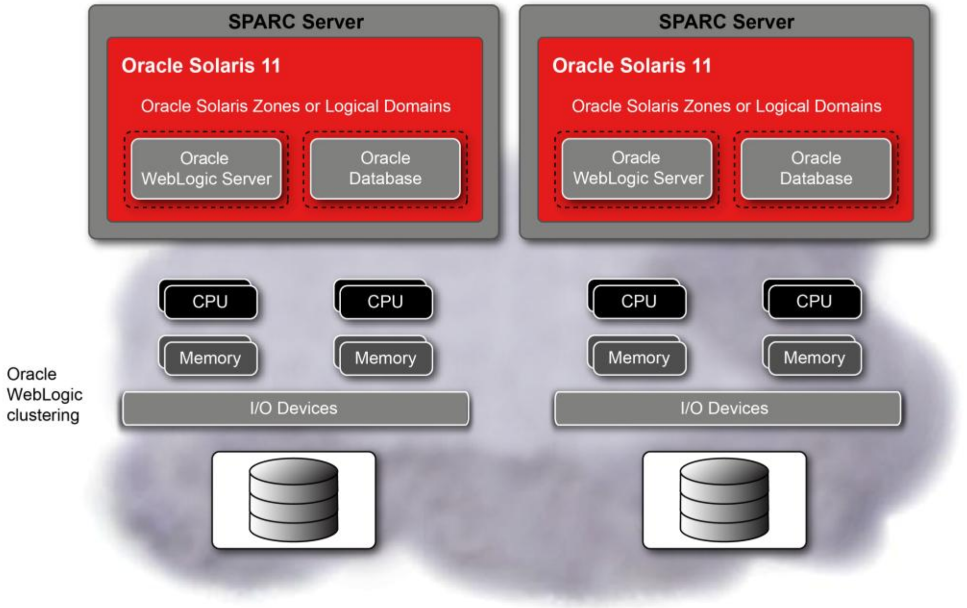

Figure 1: Oracle Optimized Solution for Secure Oracle WebLogic Server provides virtualization and clustering for scalability and high availability.

The solution as described in this document provides for several different sizing and performance options. Virtualization is employed to make efficient use of the available hardware, and both Oracle VM Server for SPARC (LDoms) and Oracle Solaris Zones have been tested. Because no significant performance differences were seen in either case, zones are illustrated as the default cases in this document for simple administration and management. Physical systems are abstracted to accommodate the different models of servers that can be substituted for varying performance requirements, as outlined later in the section on sizing.

Physical Architecture

Oracle Optimized Solution for Secure Oracle WebLogic Server is architected as a cluster of two SPARC servers (SPARC T7-1 servers, in the tested example) attached to a 10 gigabit Ethernet (GbE) network switch providing separation for public networks, cluster interconnects, and database access. In each SPARC server, one or more virtual machines (VMs) are configured to act as Oracle WebLogic Server hosts or Oracle Database servers.

Oracle WebLogic Server scales horizontally. In larger configurations, this solution architecture may consist of multiple SPARC servers attached to the 10 GbE network fabric. Implementations requiring high availability take advantage of Oracle WebLogic Server clustering technology to combine multiple SPARC servers into active-active clusters that can take over from each other in the event of a cluster member failure. The 10 GbE connectivity provides further flexibility and options for extending the function of this solution. A database tier, additional servers, or NAS options can be connected easily into this network infrastructure to provide a well-integrated full-stack solution.

Virtual Architecture

For the purposes of this document, two SPARC T7-1 servers constitute the base configuration. Using Oracle Solaris Zones (or, optionally, LDoms), each SPARC server is then logically divided into two separate VMs, as shown in Figure 2. Each VM hosts one or more instances of Oracle WebLogic Server or Oracle Database. The CPU, memory, and network I/O resources of the SPARC server are suitably allocated to help ensure that each individual VM has sufficient resources available to it.

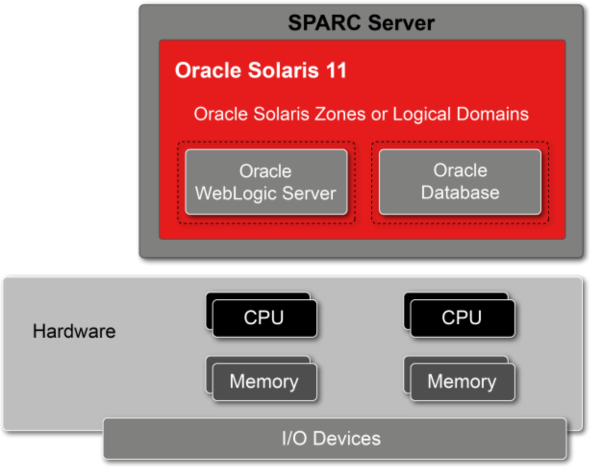

Figure 2: Instances of Oracle WebLogic Server run in separate zones or LDoms on the SPARC T7-1 server with the option to allocate the appropriate amounts of CPU, memory, and I/O resources as necessary for optimal performance.

Given the negligible overhead and ease-of-use characteristics of zones and LDoms, it is both efficient and convenient to separate multiple application server instances by installing them into different VMs. This virtualized architecture provides flexible resource allocation, security, and scalability, as well as power and space savings afforded by consolidation onto one or more high-performance servers such as the SPARC T7-1 server. Additionally, when correctly configured, both zones and LDoms are a recognized license boundary for Oracle software licensing purposes, which can enable substantial cost savings.

Extending scale and increasing resiliency from this basic unit is a matter of adding more server units and interconnecting them via the 10 GbE switch, as shown in Figure 3. Once two or more Oracle WebLogic Server instances are available, clustering can be configured to manage failover between Oracle WebLogic Server instances running on separate servers, providing significant high availability benefits.

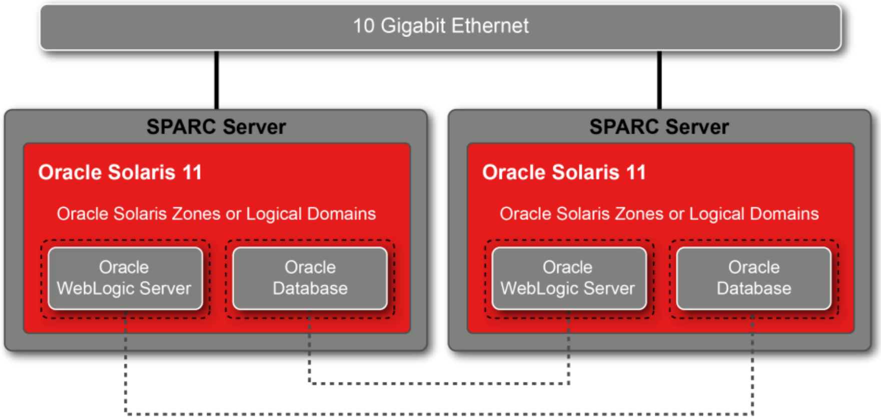

Figure 3: Oracle WebLogic Server clustering can be configured for increased availability and scalability of the solution.

Tuning Guidelines

The tuning described below was performed on the SPARC T7-1 servers used to deploy Oracle WebLogic Server in Oracle's test environment.

The following tuning was performed in the `/etc/system` file:

```
set autoup = 345600

set rlim_fd_max – 131072
```

The following network tuning was performed using `ndd`:

```
ndd -set /dev/tcp tcp_conn_req_max_q 40000

ndd -set /dev/tcp tcp_conn_req_max_q0 40000

ndd -set /dev/tcp tcp_xmit_hiwat 1048576

ndd -set /dev/tcp tcp_recv_hiwat 1048576

ndd -set /dev/tcp tcp_smallest_anon_port 4096

ndd -set /dev/tcp tcp_naglim_def 1
```

The following kernel tuning was performed in the `/kernel/drv/ixgbe.conf` file:

```
/kernel/drv/ixgbe.conf

rx_ring_size = 2048
```

Also, for each port-specific *ixgbe* device, the following script was used to enable jumbo frames and configure interrupt throttling as needed for the best performance for benchmarking.

```
# Interfaces to drivers (in this example only ports 2, 3, 4 and 5 are required)
for I in 4 5 2 3
do
  $sudo dladm set-linkprop -p mtu=9000 ixgbe${I}
  $sudo ndd -set /dev/ixgbe${I} intr_throttling 2000

done
```

Performance Expectations

In the process of testing Oracle WebLogic Server, Oracle test engineers looked at system resource utilization and throughput metrics as they scaled the number of transactions upward. The performance results from this test were used to determine the recommended sizing guidelines for different configurations. Using the typical performance testing is not possible with a clustered configuration as these benchmarks are not designed to work with the networking requirements of clustered Oracle WebLogic instances. Instead, performance was tested in standalone configurations with zones and LDoms, and found to be comparable to the most recent world-record performance results for Oracle WebLogic Server.

In high availability cluster configurations, the most important metric is often failover times in the event of a cluster member failure. In testing conducted by Oracle, all tests resulted in a maximum failover time of no more than half a second. In standalone conventional benchmarking, it is important to examine throughput and response-time metrics together when analyzing application performance and configuration scalability. As the number of users increases, there is a corresponding increase in needed throughput. As the number of transactions increases, response time must remain within acceptable bounds. The average observed latency during benchmark testing was less than 0.170 seconds per transaction, demonstrating the solution’s ability to handle large enterprise-level workloads with outstanding user response time.

Ultimately, the benchmark tests distill into one standardized throughput score known Enterprise Java Operations Per Second (EjOPS). This score is an objective and realistic evaluation of a system’s performance running a complex Java application. A similar benchmarked configuration of Oracle WebLogic Server on a specifically tuned SPARC T7-1 server with Oracle Database running on another SPARC T7-1 server has achieved a world record for a single-socket server. It is important to note that benchmark tunings of Oracle WebLogic Server might not represent the best tuning and performance characteristics for most real-world deployments. The simple tunings used in Oracle Optimized Solution for Secure Oracle WebLogic Server are a reduced set of more-conservative tunings that still achieve approximately 80 percent of the performance of an extremely optimized benchmark configuration on SPARC T7-1 servers. These results easily surpass earlier performance achievements on dual-socket SPARC T5 processor–based servers, four-socket IBM Power 8 servers, and dual-socket x86 servers, demonstrating the inherent high performance available from Oracle WebLogic Server when deployed on SPARC M7 processor–based servers. Figure 4 illustrates a further significant benefit of the SPARC T7-1 server solution. Only the SPARC T7-1 server had security features enabled to allow world-record performance with end-to-end security. This level of security was not attempted by the competing platforms due to the overhead it would have imposed.

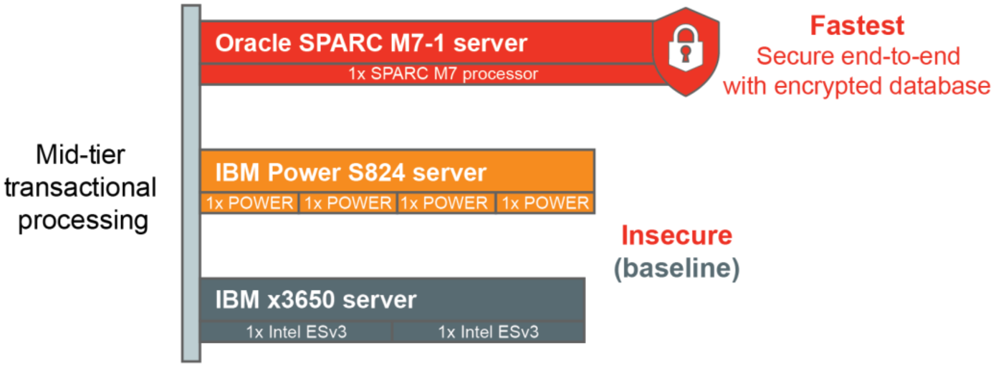

Figure 4: The SPARC T7-1 server set a world record with the added benefits of full end-to-end encryption for Oracle WebLogic Server (based on posted results for SPECjEnterprise 2010, see www.spec.org for more information).

CPU and Memory Utilization

Table 1 shows CPU and memory utilization for the components of Oracle Optimized Solution for Secure Oracle WebLogic Server. Results are shown for six configurations, differing in workload capacity. As a best practice, CPU utilization for running Oracle WebLogic Server is kept to a maximum rate of 80 percent so that performance spikes are accommodated. Likewise, memory utilization scales as the number of transactions increases.

TABLE 1. CPU AND MEMORY UTILIZATION FOR SIX CONFIGURATIONS.

	ENTRY LEVEL	SMALL	MEDIUM 1	MEDIUM 2	LARGE	EXTRA LARGE
CPU Utilization	78%	78%	78%	80%	80%	80%
Memory Utilization	90 GB	150 GB	200 GB	200 GB	250 GB	390 GB

These results were used to help determine the recommended memory sizing and guide the choice of SPARC servers, with numbers indicating CPU and memory utilization by Oracle WebLogic Server and Oracle Database instances. In each case, the memory configured in the server should comfortably exceed the total memory utilization of all zones and LDoms by at least 20 percent for consistent high performance. If additional consolidation or virtualization is performed, that must also be taken into account.

Sizing and Role Guidelines

Based on testing performed by Oracle engineers, the sizing guidelines in Table 2 represent a range of configurations from small to extra-large. These configurations are based on the expected number of transactions on Oracle WebLogic Server and are sized accordingly to provide the best performance while keeping costs in mind. Additional compute and memory capacity is available to handle peaks in utilization in all configurations.

These sizing guidelines serve as starting points when planning an Oracle WebLogic Server deployment on SPARC servers. The architecture is flexible and highly scalable, providing an easy upgrade path if workload requirements increase.

TABLE 2. SERVER SIZING FOR CLUSTERED HIGH AVAILABILITY PERFORMANCE.

	ENTRY	SMALL	MEDIUM 1	MEDIUM 2	LARGE	EXTRA LARGE
Transactions per second	5,000/sec	10,000/sec	21,000/sec	25,000/sec	50,000/sec	100,000/sec
Server	2x SPARC T7-1 servers	2x SPARC T7-1 servers	2x SPARC T7-1 servers	2x SPARC T7-2 servers	2x SPARC T7-4 servers	2x SPARC M7-8 servers
Cores per Oracle WebLogic Server instance *	8	16	32	48	64	128
Memory per node	128 GB	256 GB	512 GB	512 GB	1024 GB	1024 GB

***Note:** Only a portion of the processing power available on the SPARC M7 processor–based platform is required for some of the recommended configurations. Using suitable partitioning with LDoms or zones with resource capping can significantly reduce the cost of a smaller deployment.*

Security: SPARC Processor Cryptography Acceleration

Given escalating security challenges, encryption is increasingly important throughout modern enterprise environments. Unfortunately, merely adding encryption can quickly overburden existing production systems. For instance, simply using traditional encryption methods such as HTTPS (SSL) encryption at the web tier to secure server-to-browser (client) connections can place an additional 20 percent overhead on conventional CPU resources—essentially robbing an ordinary server of its performance value.

As a consequence, specialized, expensive cryptography cards or network appliances are often used to offload the additional workload imposed by cryptography. However, both these approaches impose penalties of their own. A cryptography card generally adds complexity, cost, and a higher power profile to a computing environment. It also increases traffic to and from the card on the system bus, imposing a system-wide performance penalty and potentially creating a system bottleneck. Using a network appliance to intercept inbound SSL traffic, strip out the encryption, and then pass the workload “in the clear” to the application introduces problems with increased resources (electricity, cooling, and footprint) and can present security compliance issues as well as introducing further complexity to the solution. Both approaches to mitigating security overhead represent additional cost of acquisition and operation.

With all of Oracle’s SPARC servers, hardware cryptography acceleration is built into specialized areas of the CPU. This functionality is easily configured using a number of methods—without additional costs. Acting as a perfect complement to technology in Oracle Solaris 11, cryptographic workloads are accelerated with minimal overall system performance degradation. As a result, organizations can enable encryption by default, without concerns that it will negatively impact performance on key systems.

There are several ways to take advantage of SPARC cryptographic hardware acceleration features, but not all are recommended, many older papers refer to the use the Oracle Kernel SSL (KSSL) proxy approach. KSSL essentially acts as a two-way proxy for intercepting SSL workloads and executing the encryption and decryption using the cryptographic capabilities of the SPARC processor rather than placing that burden on the overall system. KSSL was introduced with the early days of the SPARC T2, T3 and T4 processors as a means to quickly take advantage of the cryptographic acceleration for applications, however its use is no longer recommended as more secure and higher performance options exist to take advantage of the features of the newer SPARC T5, M6 and M7 processors.

In many cases the use of low grade SSL (versions 2.0 and 3.0) is also now discouraged as a web encryption mechanism due to recent discoveries regarding its susceptibility to hacking (see CVE-2014-2566), the current recommendation is to disable SSL 2.0 and 3.0 and instead use Transport Layer Security (TLS) version 1.1 or 1.2. Use of TLS 1.1 and 1.2 requires Java JDK version 7 update 1 (or later) and that Java Secure Socket Extensions (JSSE) is enabled.

In versions of Oracle WebLogic Server 10.3.6 or 12c JSSE and JDK 7 are certified and using java startup options enables TLS functionality, and allows the minimum acceptable version of the TLS protocol can also be specified. The required JAVA_OPTIONS can be configured via environment variables for the Solaris shell where the WebLogic startup scripts will be run.

```
export JAVA_OPTIONS=-Dweblogic.security.SSL.protocolVersion=TLS1 /

-Dweblogic.security.SSL.minimumProtocolVersion=TLSv1.1
```

The Oracle HTTP Server (OHS) should also be configured to properly take advantage of TLS and this can be achieved by ensuring that OHS version 12.1.3 is the minimum version in use and that the master copy of the ssl.conf file (at DOMAIN_HOME/config/fmwconfig/components/OHS/componentName) for OHS has the following line in it.

```
SSLProtocol nzos_Version_1_1 nzos_Version_1_2
```

Once the TLS ciphers are specified as shown above the hardware accelerators will automatically be used.

For more information on enabling TLS security on Oracle WebLogic Server, refer to My Oracle Support note number 1936300.1).

SPARC Cryptography Performance

SPARC processor–based cryptographic acceleration eliminates cryptographic overhead when using the on-chip crypto acceleration features to improve SSL responsiveness. To evaluate the effectiveness of this technology, a workload can be generated using Oracle Application Testing Suite—an Oracle test and performance monitoring suite. Tests simulated 1,000 concurrent users interacting with a website supplied from the server. Each user queried the web application using secure SSL communications as many times as possible per minute, clearing caches in between queries. The workload was sustained for 10 minutes to demonstrate a continuous workload rather than a peak performance capability. This load test was not intended to push the upper limits of the server but rather to demonstrate the overhead of cryptography at a reasonable load and the effects of using hardware-assisted cryptographic acceleration.

As shown in Figure 5, the results show minimal difference in CPU utilization due to SSL overhead between the completely unsecured application versus full end-to-end SSL encryption utilizing the on-chip cryptographic acceleration. Turning on SPARC encryption yields tangible, immediate, and cost-efficient results in the form of faster, secure transactions and fast response times—all without adding any additional security equipment costs, performance penalties or changes in power usage profiles, all without elaborate system configurations.

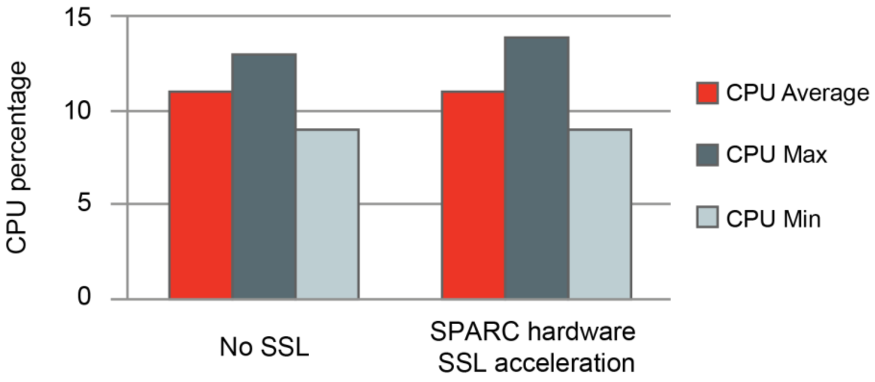

Figure 5: SPARC-based accelerated encryption results in only a minor CPU load difference from a system with no SSL encryption whatsoever, leaving CPU resources available for running the application

Understanding Oracle WebLogic Server Security

Oracle WebLogic security is a large topic and complete coverage is beyond the scope of this document. For more information, there are many specific security guides available for Oracle WebLogic Server. Please see the “For More Information” section for relevant resources. For the purposes of the Oracle Optimized Solution for Secure Oracle WebLogic Server, a cross section of best practices and industry guidelines was followed spanning the standard Oracle WebLogic Server security documents. These best practices extend to Oracle Solaris and platform security as well as securing the configuration of Oracle WebLogic Server. The US Department of Defense Security Technical Implementation Guide (STIG) recommendations for Oracle WebLogic Server 12*c* were also followed, where possible, as an industry-standard reference for security baseline configurations.

Java EE Security Feature Support in Oracle WebLogic Server

Oracle WebLogic Server supports the following security features of Java EE:

- **Java Authorization Contract for Containers (JACC) 1.4**. The JACC specification defines a contract between a Java EE application server and an authorization policy provider. All Java EE containers support this contract.
- **Java Authentication Service Provider Interface for Containers (JASPIC) 1.0**. The JASPIC specification defines a service provider interface (SPI) by which authentication providers that implement message authentication mechanisms may be integrated in client or server message-processing containers or runtimes.

Overview of the Oracle WebLogic Server Security Service

Oracle WebLogic Server includes a security architecture that provides a unique and secure foundation for applications that are available via the web. By taking advantage of the security features in Oracle WebLogic Server, enterprises benefit from a comprehensive and flexible security infrastructure. Oracle WebLogic Server security can be used standalone to secure Oracle WebLogic Server applications or as part of an enterprise-wide security management system that represents a best-in-breed security management solution.

Oracle WebLogic Server Security Framework

Figure 6 shows a high level view of the Oracle WebLogic Server Security Framework. The primary function of the framework is to provide a simplified application programming interface (API) that can be used by security and application developers to define security services. Within that context, the Oracle WebLogic Server Security

Framework also acts as an intermediary between the Oracle WebLogic Server containers (web and Enterprise Java Beans [EJB]), the resource containers, and the security providers.

Single sign-on (SSO) capability through the Oracle WebLogic Server Security Framework provides the ability to require a user to sign on to an application only once and gain access to many different application components, even though these components may have their own authentication schemes. SSO enables users to log in securely to all their applications, websites, and mainframe sessions with just one identity. The Security Assertion Markup Language (SAML) and Windows Integrated Authentication features provide web-based SSO functionality for Oracle WebLogic Server applications.

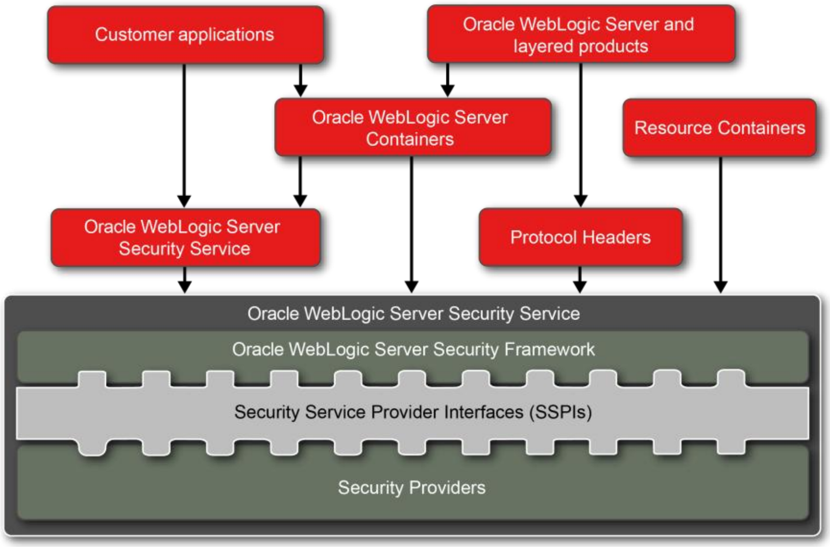
Customer applications
Oracle WebLogic Server and layered products
Oracle WebLogic Server Containers
Resource Containers
Oracle WebLogic Server Security Service
Protocol Headers
Oracle WebLogic Server Security Service
Oracle WebLogic Server Security Framework
Security Service Provider Interfaces (SSPIs)
Security Providers

Figure 6: Oracle WebLogic Server Security Framework.

The Oracle WebLogic Server Security Service architecture consists of three major components:

- **SAML Token Profile Support in Oracle WebLogic Server Web Services.** Oracle WebLogic Server web services and the Oracle WebLogic Server Security Framework support the generation, consumption, and validation of SAML 1.1 and 2.0 assertions. When using SAML assertions, a web service passes a SAML assertion and the accompanying proof material to the Oracle WebLogic Server Security Framework. If the SAML assertion is valid and trusted, the framework returns an authenticated *Subject* with a trusted principal back to the web service.
- **Security Service Provider Interfaces (SSPIs)**. Security in Oracle WebLogic Server is based on a set of Security Service Provider Interfaces (SSPIs). The SSPIs can be used by developers and third-party vendors to develop security providers for the Oracle WebLogic Server environment. SSPIs are available for Adjudication, Auditing, Authentication, Authorization, Credential Mapping, Identity Assertion, Role Mapping, and Certificate Lookup and Validation. The SSPIs allow organizations to use custom security providers for securing Oracle WebLogic Server resources. SSPIs can be used to develop custom security providers, or security providers can be purchased from third-party vendors.
- **Oracle WebLogic Server Security Providers**. Security providers are modules that “plug into” an Oracle WebLogic Server security realm to provide security services to applications. They call into the Oracle WebLogic Server Security Framework on behalf of applications. If the security providers supplied with Oracle WebLogic Server do not fully meet an organization’s security requirements, they can be supplemented or replaced with custom security providers built specifically to the needs of the organization.

Managing Oracle WebLogic Server Security

Security realms and policies offer a way to simplify secure access to resources in Oracle WebLogic Server.

Security Realms

A security realm comprises mechanisms for protecting Oracle WebLogic Server resources. Each security realm consists of a set of configured security providers, users, groups, security roles, and security policies. A user must be defined in a security realm in order to access any Oracle WebLogic Server resources belonging to that realm. When a user attempts to access a particular Oracle WebLogic Server resource, Oracle WebLogic Server tries to authenticate and authorize the user by checking the security role assigned to the user in the relevant security realm, and the security policy of the particular Oracle WebLogic Server resource.

Security Policies

Security policies replace access control lists (ACLs) and answer the question "Who has access to an Oracle WebLogic Server resource?" A security policy is created when an association is defined between an Oracle WebLogic resource and one or more users, groups, or security roles. Organizations can optionally define date and time constraints for a security policy. An Oracle WebLogic Server resource has no protection until it is assigned a security policy.

Security policies can be assigned to any of the defined Oracle WebLogic Server resources. For example, an EJB resource or a Java Naming and Directory Interface (JNDI) resource can be the target of security policies. Attributes or operations of a particular instance of an Oracle WebLogic Server resource can also be used (for example, an EJB method or a servlet within a web application). If a security policy is assigned to a type of Oracle WebLogic Server resource, all new instances of that resource inherit that security policy automatically. Security policies assigned to individual resources or attributes override security policies assigned to a type of Oracle WebLogic Server resource.

Oracle Platform Security Services

Oracle Platform Security Services provide enterprise product development teams, systems integrators (SIs), and independent software vendors (ISVs) with a standards-based, portable, integrated, enterprise-grade security framework for Java Platform, Standard Edition (Java SE) and Java EE applications. Oracle Platform Security Services provides an abstraction layer in the form of standards-based application programming interfaces (APIs) that insulates developers from security and identity management implementation details.

With Oracle Platform Security Services, developers don't need to know the details of cryptographic key management or interface with user repositories and other identity management infrastructure. Similarly, in-house developed applications, third-party applications, and integrated applications all benefit from the same uniform security, identity management, and audit services across the enterprise. Oracle Platform Security Services is available as part of Oracle WebLogic Server.

Conclusion

Driving IT forward requires cost reduction, new product innovation, and increased productivity. As the #1 application server across conventional and cloud environments, Oracle WebLogic Server 12*c* empowers data centers to achieve these goals. Oracle Optimized Solution for Secure Oracle WebLogic Server takes these capabilities to the next level by providing a best-of-breed combination of Oracle hardware, storage, and software in support of performant and highly available Oracle WebLogic Server deployments. With these advantages, organizations can deliver
next-generation applications on a mission-critical cloud platform, simplify operations with native cloud management, and accelerate time to market with a modern development platform and integrated tools.

Oracle Optimized Solution for Secure Oracle WebLogic Server provides flexibility between on-premises and third-party clouds, and is optimized for Oracle Exalogic Elastic Cloud. As the cornerstone of the Oracle cloud application foundation, Oracle WebLogic Server provides extreme cloud performance, scalability, and elasticity, and unmatched integration with Oracle Database 12*c* and its multitenant architecture. It helps increase developer productivity, including mobile application development, and provides Maven support, making Oracle the undisputed leader in the application server industry. Extensive security provided with Oracle WebLogic Server helps organizations assert control over security policies while built-in encryption in Oracle's SPARC servers helps ensure secure operation without negatively impacting performance. A range of available servers based on Oracle's SPARC M7 processor help ensure that capable platforms are available to serve a broad range of workloads.

For More Information

For more information on Oracle Optimized Solution for Secure Oracle WebLogic Server on SPARC processor-based servers, see the references listed in Table 3.

TABLE 3. REFERENCES FOR MORE INFORMATION.

Oracle WebLogic Server	oracle.com/us/products/middleware/cloud-app-foundation/weblogic/overview/index.html
Oracle's SPARC M7 processor based servers	oracle.com/servers
Oracle Solaris 11	oracle.com/us/products/servers-storage/solaris/solaris11/overview/index.htm
Oracle Database	oracle.com/us/products/database/index.html
SPECjEnterprise2010 Result	spec.org/jEnterprise2010/results/res2011q3/jEnterprise2010-20110907-00027.html
"High-Performance Security for Oracle WebLogic Server Applications Using Oracle's SPARC T-5 and SPARC M5 Servers"	oracle.com/technetwork/articles/systems-hardware-architecture/security-weblogic-t-series-168447.pdf
US Department of Defense Security Technical Implementation Guide (STIG) recommendations for Oracle WebLogic Server 12c	iase.disa.mil/stigs/Documents/u_oracle_weblogic_server_12c_v1r1_stig.zip
Oracle Fusion Middleware security blog	fusionsecurity.blogspot.com/

SPECjEnterprise2010 models contemporary Java-based applications that run on large Java EE servers backed by network infrastructure and database servers. SPEC and the benchmark name SPECjEnterprise are registered trademarks of the Standard Performance Evaluation Corporation. Results from www.spec.org as of 10/25/2015. SPARC T7-1, 25,818.85 SPECjEnterprise2010 EjOPS (unsecure); SPARC T7-1, 25,093.06 SPECjEnterprise2010 EjOPS (secure); Oracle Server X5-2, 21,504.30 SPECjEnterprise2010 EjOPS (unsecure); IBM Power S824, 22,543.34 SPECjEnterprise2010 EjOPS (unsecure); IBM x3650 M5, 19,282.14 SPECjEnterprise2010 EjOPS (unsecure).

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services

Oracle Optimized Solution for Secure Oracle WebLogic Server
October 2015